Date: August 25, 2015

To: Assistant Secretary for Indian Affairs Employees, Contractors, and Users of AS-IA Systems
Bureau of Indian Affairs Employees, Contractors, and Users of BIA Systems
Bureau of Indian Education Employees, Contractors, and Users of BIE Systems

On behalf of: Mr. Thomas D. Thompson, Deputy Assistant Secretary (Management) - Indian Affairs
Mr. Michael S. Black, Director, Bureau of Indian Affairs
Dr. Charles Roessel, Director, Bureau of Indian Education

From: Mr. Phillip L. Brinkley, Senior Advisor for Information Resources (SAIR) - Indian Affairs

Subject: CYBER HYGIENE

Recently, the President of the United States assembled his Cabinet and reiterated his continuing concerns regarding the real and serious threats to our federal networks, information systems and sensitive information. Congress is also doing their part to help agencies identify and correct vulnerabilities and weaknesses in our systems by providing funding of technical solutions through the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) capabilities. While we continue to work to implement and deploy these solutions across the Department, the Secretary and Deputy Secretary have asked the Department of the Interior, Office of the Chief Information Officer (OCIO) to help them raise awareness and attention to the President's concerns.

The OCIO asks that you remain vigilant and be extra diligent in doing your part to help protect our IT systems and information by ensuring that you consistently follow cyber hygiene best-practices as you perform your daily work to securely design, build/implement (configure, test, deploy), maintain and operate our IT systems. To remind you of some best practices that might be relevant, the Department has provided the tips to follow.

We would like to personally thank each one of you for doing your best each day to help safeguard our IT systems and information that are so vital to the continued success of our missions and our service to the public. We could not accomplish our mission without your dedication and support.

If you have questions about this information, please contact Mr. Randolph Dyer, Bureau Chief Information Security Officer (BCISO) at randolph.dyer@bia.gov.

Pertinent to IT Professionals and System Owners:

Computer and Application Hardening

Computer and application hardening is the process of enhancing the security of those information technology resources. Many systems and applications today are attacked hundreds of thousands of times each and every day. The best defense against such attacks is to ensure that computer and application hardening is a well-established practice. The following are some common hardening tips & best practices that may be applicable to the computers and applications that you are responsible for and that you may need to consider.

- Immediately change default passwords for all devices, workstations, servers, software, applications, databases, etc and remove, rename or disable as appropriate all unnecessary default accounts

- Enforce very strong passwords for all needed accounts and do not permit empty passwords
- Obtain all software, scripts, and source code from a trusted, validated and reliable source that has thoroughly inspected them for any malicious logic so as not to introduce any potential malicious code into our network or systems that might lead to their compromise
- Never access your email from a server you manage and never access your email when you are logged into your regular work computer with your privileged account so as to prevent malicious code from doing damage or propagating to other systems using your elevated access
- Never access Internet sites from a server you manage and never access those sites when you are logged into your regular work computer with your privileged account so as to prevent malicious code from doing damage or propagating to other systems using your elevated access
- Use Data Encryption for data at rest and data in motion
- Avoid using insecure protocols that transmit information or passwords in plain text
- Remove unnecessary software and services on your systems, including Php, IRC - BitchX, bnc, eggdrop, generic-sniffers, guardservices, ircd, psyBNC, and ptlink
- Disable unwanted binaries such as SUID and SGID
- Secure /tmp /var/tmp /dev/shm and sysctl.conf
- Hide BIND DNS Server Version and Apache version
- Minimize open network ports to be only what is needed for your specific circumstances
- Keep your operating system and all installed applications up-to-date, especially security patches
- Utilize security extensions if available and appropriate
- When using Linux, SELinux should be considered, weighing the enhanced security with impacts to your web hosting capabilities
- Install and run Chkrootkit and Rkhunter on your Linux server (but not at the same time) to help detect if your system has been compromised
- Install Linux Socket Monitor, which detects/alerts when new sockets are created on your system and often reveals hacker activity
- Change your administrative passwords on a regular basis and never reuse them
- Lock accounts after too many login failures since these are often illegitimate attempts to gain access to your system
- Use brute force and intrusion prevention systems
- Change the SSH port from default to a non-standard one
- Disable direct root logins and switch to root from a lower level account only when necessary
- Configure the system firewall (Iptables) or get software installed (e.g., CSF or APF) such as proper setup of a firewall itself can prevent many attacks
- Consider also using hardware and application firewalls where appropriate
- Separate partitions in ways that make your system more secure
- Maintain server logs; mirror logs to a separate log server
- Utilize a Security Information and Event Management (SIEM) solution, review security event logs daily, and investigate suspicious activity on your server - utilize enterprise

solutions to the greatest extent practicable in order to help identify threats to the entire organization/environment

- Limit user accounts to accessing only what they need; increasing access should only be done on an as-needed basis and always remove access when no longer needed
- Maintain proper backups
- Don't forget about physical server security